CMCS Security and Privacy Policy

Version 1.0

Data Security

The CMCS Service provides access control mechanisms whereby Content Providers can determine to what extent other parties can have read or write access to their Content. Content Providers are expected to become familiar with the implementation of access controls in the CMCS Service, and to take responsibility for the accessibility of their Content on the Service. The possibility exists that the CMCS Service access control mechanisms can fail. In such an event, Content could be exposed to parties unintended by the Content Provider. In the case of a breach of CMCS access controls, CMCS will make reasonable efforts to determine the nature and extent of the breach, make reasonable efforts to rectify the problem, and to notify affected parties in a timely fashion.

CMCS will make reasonable efforts to assure the robustness of the CMCS Service. CMCS will prioritize development towards the goal of preventing accidental data loss or degradation. However, data loss or degradation is always a possibility, and independent data backups are strongly advised. In the event of data loss, CMCS will make reasonable efforts to notify all parties known to be affected.

CMCS will make reasonable efforts to assure the availability of the CMCS Service. The goal of the CMCS Service is to be available 24 hours a day, 7 days a week. However, there will be occasional Service outages for scheduled maintenance; advance notice of such outages will be posted in the CMCS portal. CMCS will attempt to minimize the duration and frequency of outages.

User Information

Users are required to register with the CMCS Service prior to its use by providing name and valid email address. Other information may be provided by users on an optional basis, including their workplace, occupation, phone number, and their areas of scientific endeavor or expertise.

Users' information will not be shared with any entities outside of CMCS except as required by law, regulation, court or governing agency directive or as the result of security investigations.

Data Privacy

Content will not be shared with any entities outside of CMCS who have not signed the User Agreement except as required by law, regulation, court or governing agency directive or as the result of security investigations.

CMCS administrators have access to Content for reasons of security and to determine whether the Content serves the Purpose defined in the CMCS Content Provider Agreement.

While the CMCS reserves the right to review any part of the Content store, CMCS does not perform any scheduled comprehensive Content review. When discovered, non-conforming data will be removed from the CMCS Service. CMCS bears no liability for the presence of non-conforming data on the CMCS Service.

Intellectual Property and Licenses

Content found through the service may be protected by copyright or other proprietary rights. Content that appears in the CMCS Service without an explicit License is assumed to copyrighted by its contributor.

Content derived automatically from specific contributed Content via the CMCS Service infrastructure (including annotation and translations) are considered to be subject to the License of the original Content.